UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/554,518	05/11/2000	LYNN D SPRAGGS	PA1317US	2076

7590 02/11/2004

Lynn D. Spraggs
8604 Kalavista Drive
Vernon B.C., V1B 1K3
CANADA

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	8

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

P24

Office Action Summary	Application N .	Applicant(s)	
	09/554,518	SPRAGGS, LYNN D	
	Examiner	Art Unit	
	LEYNNA T. HA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the corresp ndence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-41 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-41 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. **Claims 1-41 have been examined.**

2. **Claims 1-3 and 7-16 are rejected under 35 U.S.C. 112, 2nd paragraph.**

3. **Claims 1-41 is rejected under 35 U.S.C. 102(e).**

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claims 1-3 and 7-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Claim 1, states "to decrypt an encrypted data file provided by the user into the encryption key" is vague. It is unclear what is "into the encryption key" after decrypting the encrypted data file. Is this a process of generating an encryption key?

Claim 7, states "decrypting the encrypted data file using the password, into an authenticated encryption key" is vague. It is unclear what is "into the authenticated encryption key" after decrypting the encrypted data file. Does decrypted the encrypted data file become the authenticated encryption key?

Claim 13, states "to decrypt an encrypted data file provided by the user into an authenticated encryption key" is vague. It is unclear what is "into the encryption key" after decrypting the encrypted data file. By decrypting the encrypted data file, does this lead into generating or becoming a different key? All other claims are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 1-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Thomlins n, Et Al. (US 6,532,542).

As p r claim 1:

Thomlinson teaches a system for authenticating an encryption key of a user comprising a decrypt engine for using a password (col.10, lines 1-6) provided by the user to decrypt an encrypted data file (col.10, lines 12-15) provided by the user into the encryption key of the user (col.10, lines 15-25).

As per claim 2:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 3:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 7:

Thomlinson teaches a method for providing an authenticated encryption key of a user, comprising the steps of providing an encrypted data file (col.10, lines 43-45), providing a password (col.10, lines 1-3), and decrypting the encrypted data file using the password into an authenticated encryption key of user (col.11, lines 2-25).

As per claim 8:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 9:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 10:

The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 11:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein the method includes a scanner as one of the input devices used to enter commands and information to the computer (col.5, lines 24-28) and biometric authentication procedures (col.9, lines 47-54). Thus, the Examiner asserts it is inherent that Thomlinson teaches the method of generating biometric data of the user by scanning the biometric feature of the user and comparing the generated biometric data of the user to the data derived from the encrypted data file to authenticate the encryption key of the user (col.10, lines 30-42).

As per claim 12:

The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 13:

Thomlinson discloses a computer accessible medium comprising program instructions (col.4, lines 35-36) for providing an authenticated

encryption key of a user by using a password provided by the user to decrypt an encrypted data file provided by the user into an authenticated encryption key of the user (col.10, lines 1-46).

As per claim 14:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 15: See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 16:

As rejected with the same rationale of claim 14 and further includes Thomlinson discussing the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 17:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input device used to enter commands and information such as a keyboard to receive a password from a user (col.5, lines 24-28). Further, Thomlinson include memory for storing an encrypted data file including an encryption key of the

user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) and thereby generating an authenticated the encryption key of the user (col.10, lines 15-25).

As per claim 18:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 19:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 20:

The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 21: See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 22:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein the method includes a scanner as one of the input devices used to enter commands and information to the computer (col.5, lines 24-28) and biometric authentication procedures (col.9, lines 47-54). Thus, the Examiner asserts it is inherent that Thomlinson teaches the method of generating biometric data of the user by

scanning the biometric feature of the user such as the fingerprint of the user. See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 23: See col.11, lines 7-12; discussing the server configured to receive data encrypted using the authenticated encryption key.

As per claim 24:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input device used to enter commands and information such as passwords from the user (col.5, lines 24-28). Further, Thomlinson include an RF smart card (col.7, lines 2-10) for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) and thereby generating an authenticated the encryption key of the user (col.10, lines 15-25).

As per claim 25:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 26:

The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 27:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input devices used to enter commands and information such as a keyboard for entering passwords from the user and a scanner (col.5, lines 24-28) for biometric authentication procedures (col.9, lines 47-54). Further, Thomlinson include an RF smart card (col.7, lines 2-10) for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) and thereby generating an authenticated the encryption key of the user (col.10, lines 15-25). Although, Tomlinson did not discuss a biometric reader, however, the Examiner asserts it is inherent to include a biometric reader if Tomlinson discloses biometric authentication procedures.

As per claim 28:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input device used to enter commands and information such as a keyboard to receive a password from a user (col.5, lines 24-28). Further, Thomlinson include memory for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) and thereby

generating an authenticated the encryption key of the user (col.10, lines 15-25).

As per claim 29:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 30:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 31:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input devices used to enter commands and information such as a keyboard for entering passwords from the user and a scanner (col.5, lines 24-28) for biometric authentication procedures (col.9, lines 47-54). Although, Tomlinson did not discuss a biometric reader, however, the Examiner asserts it is inherent to include a biometric reader if Thomlinson discloses biometric authentication procedures. Thomlinson includes memory for storing an encrypted encryption key and biometric data of the user (col.11, lines 7-12). Further, Thomlinson discloses a master key used to decrypt an appropriate item key and corresponding item authentication key. See col.10, lines 2-21; discussing the password or other logon procedure where the Examiner asserts Thomlinson

inherently includes password and biometric verification as the logon procedure (col.9, lines 52-54).

As per claim 32: See col.10, lines 2-6 and lines 40-42; discussing the password or other logon procedure where the Examiner asserts Thomlinson inherently includes password and biometric verification as the logon procedure (col.9, lines 52-54).

As per claim 33:

The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 34:

Thomlinson includes memory for storing an encrypted encryption key (col.10, lines 35-36) and includes an input devices used to enter commands and information such as a keyboard for entering a password from the user (col.5, lines 24-28) that is required the use of the password to decrypt the encrypted encryption key to a decrypted encrypting key (col.10, lines 18-23).

As per claim 35:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 36:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 37:

The Examiner ascertains that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 38: See col.10, lines 2-6 and lines 40-42; discussing the password or other logon procedure where the Examiner asserts Thomlinson inherently includes password and biometric verification as the logon procedure (col.9, lines 52-54).

As per claim 39:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein the method includes a scanner as one of the input devices used to enter commands and information (col.5, lines 24-28) for biometric authentication procedures to the computer (col.9, lines 47-54). Thus, the Examiner asserts it is inherent that Thomlinson teaches the method of generating biometric data of the user by scanning the biometric feature of the user such as the fingerprint of the user. See col.10, lines 2-6 and lines 40-42; discussing the password or other logon procedure where the Examiner asserts Thomlinson inherently includes password and biometric verification as the logon procedure (col.9, lines 52-54) and comparing or verifying process by decrypting the encrypted encryption key (col.11, lines 15-18).

As per claim 40:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 41: See col.10, lines 20-45; discussing using the decrypted encryption key to encrypt the data.

Conclusion

Please refer to Thomlinson, Et Al.: see col.1, ET SEQ.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

LHa

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
09/554,518